(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 197 24 901 A 1**

(51) Int. Cl.[6]:
H 04 Q 7/32
H 04 Q 7/38
H 04 L 12/16

(21) Aktenzeichen: 197 24 901.9
(22) Anmeldetag: 12. 6. 97
(43) Offenlegungstag: 17. 12. 98

(71) Anmelder:
Siemens Nixdorf Informationssysteme AG, 33106 Paderborn, DE

(74) Vertreter:
Epping, W., Dipl.-Ing. Dr.-Ing., Pat.-Anw., 82131 Gauting

(72) Erfinder:
Wiehler, Gerhard, 82223 Eichenau, DE

(56) Entgegenhaltungen:

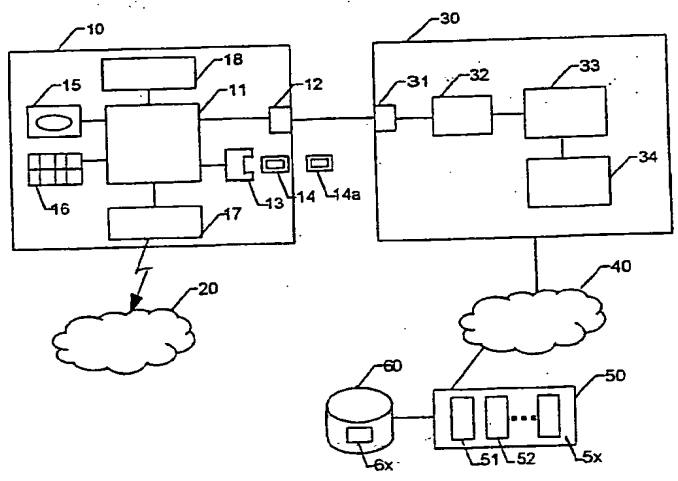
DE	1 95 38 842 A1
DE	2 95 20 925 U1
DE	94 15 302 U1
GB	22 74 960 A
US	44 55 226
WO	95 15 065 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Mobilfunktelefon sowie solche mit gekoppeltem Rechner für Internet- bzw. Netzanwendungen und Verfahren zum Betreiben einer solchen Gerätekombination

(57) Anschluß der Kontaktiereinheit 13 des Mobilfunktelefons 10 über eine Steuereinheit 11 an die Anschlußschnittstelle 12 für den Rechner 30, so daß Daten zwischen einer Chipkarte 14/14a und der Anschlußschnittstelle 12 über die Steuereinheit austauschbar sind. Bei Kopplung mit einem Rechner 30 ist das Mobilfunktelefon 10 als Kartenterminal betreibbar, so daß vom Rechner 30 aus über ein Kommunikationsnetz 40 eine Inanspruchnahme der Netzdienste von Dienstanbietern 50 möglich ist. Chipkartenanwendungen z. B. für die gegenseitige Client-Server-Authentisierung, für die Verifikation von Zugriffsrechten, für die digitale Signatur sensibler Daten, für die Erzeugung von Schlüsseln zur Verschlüsselung von Daten, für den Beweis eines Bestellvorganges, für die Bezahlung aus einer elektronischen Börse usw.



DE 197 24 901 A 1

DE 197 24 901 A 1

NSDOCID: <DE__19724901A1_I_>

Beschreibung

Die Erfindung betrifft Anordnungen und Verfahren für die Nutzung von im Internet oder in anderen Netzen angebotenen Leistungen, die hohe Sicherheitsanforderungen stellen.

Mobilfunktelefone werden im wesentlichen für die Sprachübertragung in Mobilfunknetzen benutzt. Das im Mobilfunktelefon integrierte sogenannte SIM-Modul bzw. die integrierte Chipkarte dient zur Authentisierung des Mobilfunktelefons als ein für den Mobilfunk berechtigtes Gerät und enthält Schlüssel für die Verschlüsselung der ausgesandten Sprachinformation bzw. für die Entschlüsselung der empfangenen Sprachinformation.

Rechner, wie z. B. Personalcomputer oder Laptops, die einen Festnetz- oder Mobilnetzanschluß aufweisen, sind in der Lage, z. B. mittels http-Protokoll, Internetanwendungen zu nutzen. Bei besonders sicherheitsrelevanten Vorgängen, wie z. B. bei Bestellungen und Zahlungen, werden Chipkarten verwendet, die über einen am Rechner angeschlossenen Chipkartenleser die jeweiligen Transaktionen steuern. Die Verbindung mit einem Mobilfunknetz kann dabei auch über ein mit einem Datenanschluß-ausgerüsteten Mobilfunktelefon erfolgen – man siehe z. B. "PC Professionell", März 1994, Seiten 253–260 oder "Cash Flow", 2/95, Seiten 140, 141.

Mögliche Anwendungen in Verbindung mit einer Chipkarte sind z. B. Authentisierung, Erzeugung von digitalen Signaturen, Kredit-/Debitkartenanwendungen, elektronische Geldbörse.

Eine besonders hohe Sicherheit kann durch asymmetrische kryptographische Verfahren erreicht werden, bei denen der private Schlüssel in der Chipkarte nicht auslesbar gespeichert ist und entsprechende Krypto-Verfahren in der Chipkarte nicht manipulierbar durchgeführt werden. Chipkarten-Bausteine für derartige Anwendungen sind heute auf dem Markt verfügbar, z. B. der Baustein SLE 44CR80S der Siemens AG.

Aufgabe der Erfindung ist es, den Anwendungsbereich des Mobilfunktelefons so zu erweitern, daß in Verbindung mit einem Rechner gesicherte Transaktionen in den ansteuerbaren Netzen möglich sind.

Dieses wird einerseits gemäß Anspruch 1 dadurch erreicht, daß das Mobilfunktelefon in der Weise erweitert wird, daß es zusätzlich als Kartenterminal für einen Rechner verwendbar ist, indem die Kontaktiereinheit über eine Steuereinheit mit der Anschlußschnittstelle für den Rechner koppelbar ist. An diese Steuereinheit können auch die übrigen für den Mobilfunkverkehr benötigten Bauteile angeschlossen sein, um weitere Steuerfunktionen zu ermöglichen.

Weiterhin ermöglicht die Verwendung eines solchen erweiterten Mobilfunktelefons gemäß Anspruch 3 in Verbindung mit einem Rechner, der unabhängig vom Funkteil des Mobilfunktelefons an ein Kommunikationsnetzwerk in bekannter Weise angeschlossen ist, daß ein Mobilfunktelefon-Inhaber ortsunabhängig von jedem beliebigen Standard-Rechner aus persönliche oder öffentliche Netzdienste, z. B. über das Internet, in Anspruch nehmen kann, die an die Sicherheit hohe Anforderungen stellen, ohne daß diese Standardgeräte über Chipkarten-Leseeinrichtungen verfügen müssen.

Weiterbildungen der Erfindung beziehen sich auf Verfahren zum Betreiben einer derartigen Gerätekombination. Diese betreffen u. a. das Betriebsbereitschalten des Mobilfunktelefons als Kartenterminal, das neben der Abwicklung von Netzdiensten in der üblichen Weise auch Verschlüsselungen bzw. Entschüsselungen in an sich bekannter Weise ermöglicht.

Besondere Vorteile ergeben sich daraus, daß hochsensible Daten, wie z. B. die persönliche Geheimzahl PIN oder Geldbeträge am Mobiltelefon mit der Tastatur eingegeben und unverschlüsselt angezeigt werden können, bevor sie verschlüsselt an den Rechner weitergeleitet werden. Damit werden Eingaben über die Rechnertastatur vermieden, so daß Viren im Rechner die Eingaben nicht verfälschen können.

Auch besteht in vorteilhafter Weise die Möglichkeit, Kontrollwörter über das Mikrofon als Berechtigungsnachweis einzugeben, die dann digitalisiert an eine Kontrollinstanz im Kommunikationsnetz weitergeleitet und mit einem Referenzmuster verglichen werden. Auf diese Weise kann die Identität eines Benutzers zusätzlich anhand eines persönlichen biometrischen Merkmales verifiziert werden, was erhöhten Sicherungsanforderungen gerecht wird.

Weiterhin können auch Daten und/oder Steuerinformationen vom Rechner über die Anschlußschnittstelle an den Speicher im Mobilfunktelefon übertragen und dort abgespeichert werden. Damit ist es möglich, Daten auf der Chipkarte zu ändern oder zu speichern. Bei diesen Daten kann es sich z. B. um Schlüssel für die Verschlüsselung bzw. Entschlüsselung oder um einen Geldbetrag für eine Geldkarte handeln. Letztere eröffnet zudem die Möglichkeit eines Kartentelefons, indem beim Betrieb als Telefon ankommende Gebührenimpulse eine Abbuchung des jeweils entsprechenden Geldbetrages bewirken.

Einzelheiten der Erfindung seien nachfolgend anhand eines in der Zeichnung dargestellten Ausführungsbeispieles näher erläutert. Im einzelnen zeigen

Fig. 1 eine schematische Übersicht eines Rechners mit Netzkopplung und angeschlossenem Mobilfunktelefon als Kartenterminal für die Inanspruchnahme von Netzdiensten und

Fig. 2 eine schematische Darstellung einer Chipkarte für verschiedene Anwendungen.

Bei der Darstellung von **Fig.** 1 ist ein Mobilfunktelefon **10** über eine Standardschnittstelle **12**, z. B. RS232, an einen Rechner **30** in Form eines üblichen PC angeschlossen. Die Schnittstelle **12** ist innerhalb des Mobilfunktelefons **10** mit einer Steuereinheit **11** verbunden, an die außerdem eine Kontaktiereinheit **13** für das SIM-Modul/die Chipkarte **14/14a**, eine Anzeige **15**, eine Tastatur **16**, ein Sprach- und Funkmodul **17** sowie ein Speicher **18** angeschlossen ist. Das Sprach-und Funkmodul **17** hat dabei in üblicher Weise Zugang zum Mobilfunknetz **20**.

Vom Rechner **30** sind lediglich die Anschlußschnittstelle **31** für das Mobilfunktelefon **10** mit dem zuständigen Treiber **32** gezeigt sowie ein sogenannter Browser **33** und Rechneranwendungen **34** für die Inanspruchnahme von Netzdiensten, beispielsweise im Internet, angedeutet, die über das Kommunikationsnetz **40** in Verbindung mit einem entsprechenden Anbieter **50**, z. B. in Form eines sogenannten Servers, ausgeführt werden können.

Auf dem SIM-Modul oder der Chipkarte **14** bzw. **14a** sind die mit Schlüssel zugänglichen Anwendungen gespeichert. Für die verschiedenen Anwendungen können individuelle Chipkarten vorgesehen werden. Es können aber auch, wie **Fig.** 2 zeigt, die Mobilfunk-Anwendungen für GSM/DCS **141** sowie die verschiedenen Internet-/Netzanwendungen **142**, **143**, **14x** mit ihren unterschiedlichen Schlüsseln auf einer Chipkarte gespeichert sein.

Vor Nutzung eines der Netzdienste ist eine entsprechende Chipkarte auszuwählen und in die Kontaktiereinheit **13** des mit dem Rechner gekoppelten Mobilfunktelefons **10** einzusetzen. Außerdem ist der das Mobilfunktelefon **10** als Kartenterminal über die Anschlußschnittstelle **31** steuernde Treiber **32** mit der entsprechenden Treibersoftware zu laden.

Dies kann von einer Diskette aus erfolgen. Um jedoch Manipulationen am Treiber **32** auszuschließen, ist es zweckmäßig, daß die z. B. mit einem privaten Schlüssel des Mobilfunknetz-Betreibers signierte Treibersoftware von einem entsprechenden Server auf Anforderung vom Rechner **30** aus über das Kommunikationsnetz **40** in den Treiber **32** geladen wird. Danach kann dann automatisch eine Verifikation der Treibersoftware anhand eines entsprechenden und sich auf der Chipkarte **14/14a** in einem Anwendungsbereich, z. B. **14x**, befindlichen öffentlichen Schlüssel des Mobilfunknetz-Betreibers durchgeführt werden.

Die Treibersoftware arbeitet zweckmäßig entsprechend einem bereits festgelegten Standard, wie z. B. ISO 7816-3 und der von der PC/SC-Workgroup gemeinsam mit Microsoft festgelegten ICC Spezifikation (http//:www.smartcard-sys.com)

Die Netzanwendung kann im Rechner **30**, beispielsweise durch Aufrufen des Browsers **33** und Eingabe eines sogenannten "uniform resource locator" URL gestartet werden. Damit wird über das Netz **40** eine Verbindung zum Dienstanbieter **50** aufgebaut, und es können die gewünschten Dienste **51, 52, . . ., 5x** in Anspruch genommen werden. Das angeschlossene Mobilfunktelefon **10** bzw. die Steuereinheit **11** verhält sich dabei wie ein übliches Kartenterminal. Abhängig von den vom Dienstanbieter **50** bereitgestellten Diensten **51, 52, . . ., 5x** sind Chipkartenanwendungen **142, 143, . . ., 14x** auswählbar und ausführbar, z. B. für die gegenseitige Client-Server-Authentisierung, für die Verifikation von Zugriffsrechten, für die digitale Signatur sensibler Daten, für die Erzeugung von Schlüsseln zur Verschlüsselung von Daten, für den Beweis eines Bestellvorganges, für die Bezahlung aus einer elektronischen Börse.

Gegenüber einem herkömmlichen Chipkartenleser ermöglicht die Erfindung zusätzliche Funktionen des Mobilfunktelefons, die eine erheblich höhere Sicherheit gewährleisten:

Am Internet angeschlossene Rechner sind prinzipiell aus dem Internet eingeschleusten Viren ausgesetzt. So kann z. B. ein Kontoüberweisungsbetrag, der über die Rechnertastatur eingegeben wird, durch einen solchen Virus verfälscht werden, bevor die Transaktion mit dem Internetserver korrekt abgeschlossen ist.

Mit einem Mobilfunktelefon als Kartenterminal kann diese Manipulation dadurch verhindert werden, daß von der Rechner-/Server-Anwendung veranlaßt wird, sensible Daten, wie z. B. Überweisungsbeträge, über die Tastatur **16** des Mobilfunktelefons **10** einzugeben. Der Steuereinheit **11** wird dies über einen Code mitgeteilt, wodurch die eingegebenen Daten einerseits an der Anzeige **15** unverschlüsselt wahrgenommen und überprüft werden können. Andererseits werden diese Daten durch eine Chipkartenanwendung **14x** verschlüsselt oder signiert und an den Rechner **30** bzw. den zuständigen Server zur weiteren Verarbeitung übergeben.

In gleicher Weise kann bei Eingabe einer persönlichen Geheimzahl PIN, welche durch eine Rechner-/Netz-Anwendung angefordert wurde, die an der Tastatur **16** eingegebene PIN in der Chipkarte verschlüsselt werden, bevor sie an die Rechner-/Netz -Anwendung weitergeleitet wird.

Anwendungen mit höchsten Sicherheitsanforderungen erfordern oftmals eine Authentisierung auf Basis biometrischer Merkmale. Mit der hier dargestellten Erfindung läßt sich dies folgendermaßen realisieren:

Eine Anwendung **5x** fordert nach erfolgreicher gegenseitiger Client-Server-Authentisierung auf Basis asymmetrischer Krypto-Verfahren den Benutzer als sogenannten Client auf, eine Sprechprobe abzugeben, z. B. ein vereinbartes Kennwort dreimal hintereinander in das Mikrofon **17** des Mobilfunktelefons **10** zu sprechen. Die Steuereinheit **11** leitet dann, beispielsweise veranlaßt durch einen von der Anwendung **5x** bzw. vom Browser **33** übertragenen Steuercode, den digitalisierten Sprachstrom in Form eines Bitstrings an die zuständige Anwendung, z. B. **5x**, weiter. Diese extrahiert aus dem empfangenen Bitstring die persönlichen Sprachmerkmale und vergleicht diese mit z. B. auf Plattenspeichern **60** abgelegten Referenzmustern **6x**, um die Identität des Benutzers anhand seiner Sprechproben zu verifizieren.

Die Erfindung schließt auch ein, daß im Rahmen einer Rechneranwendung **34** von einem Internet-Server in den Rechner **30** geladene Daten, wie z. B. Telefonlisten, Adressenlisten, Umsatzdaten, Preislisten, in den Speicher **18** des Mobilfunktelefons **10** geladen und auf der Anzeige **15** dargestellt werden können, wobei durch die Tastatur **16** eine Auswahl möglich ist.

Bei einer weiteren Rechneranwendung **34** können am Mobilfunktelefon **10** eingetastete oder eingesprochene, digitalisierte Daten in den Rechner **30** übertragen und dort oder in einem Netzserver weiterverarbeitet bzw. später oder von anderen Personen abgerufen werden.

Weiterhin ist es möglich, daß – angestoßen durch eine Rechneranwendung **34** – über die Anschlußschnittstelle **31/12** in den Speicher **18** des Mobilfunktelefons **10** Programme geladen werden können, die in der Steuereinheit **11** zeitlich entkoppelt zum Ablauf gebracht werden können.

Schließlich können auch Anwendungen/Schlüssel – angestoßen durch eine Rechneranwendung **34** – auf der Chipkarte selbst geändert, gelöscht oder geladen werden.

In allen Fällen kann die Übertragung von Daten, Programmen oder Anwendungen zwischen dem Mobilfunktelefon **10** bzw. der Chipkarte **14/14a** und dem Rechner **30** bzw. dem Netzserver integritätsgesichert oder verschlüsselt erfolgen. Die hierfür notwendigen Schlüssel sind entweder auf der Chipkarte bereits gespeichert oder werden vorher zwischen Rechner-/Netzserver-Anwendung und Chipkarte z. B. nach dem Diffie-Hellman-Verfahren ausgetauscht. Darüberhinaus kann das Mobilfunktelefon **10** ganz allgemein in analoger Weise für die Verschlüsselung bzw. Entschlüsselung von Daten verwendet werden.

Eine weitere Ausprägung der Erfindung besteht in der gemeinsamen Nutzung einer Chipkartenanwendung in GSM – und Festnetzen. Ein Beispiel hierfür ist die elektronische Geldbörse. Sie kann z. B. als Anwendung **14x** auf der im Mobilfunktelefon **10** eingelegten Chipkarte **14/14a** über eine Rechner-/Netz-Anwendung **33/34/5x** aufgeladen werden und später während eines GSM-Telefongespräches, z. B. durch einen von der Funkvermittlungszentrale gesendeten Impuls in regelmäßigen Zeitabständen– entsprechend den entfernungsabhängigen Tarifen – dekrementiert werden. Derartiges "vorausbezahltes" Telefonieren reduziert das Betrugsrisiko, dem Mobilfunkbetreiber heute vielfach ausgesetzt sind, erheblich.

Patentansprüche

1. Mobilfunktelefon (**10**) mit Kontaktiereinheit (**13**) für eine Chipkarte (**14, 14a**) als Berechtigungsnachweis für den Mobilfunkverkehr und einer Anschlußschnittstelle (**12**) für einen Rechner (**30**), **dadurch gekennzeichnet**, daß die Kontaktiereinheit (**13**) über eine Steuereinheit (**11**) auch mit der Anschlußschnittstelle (**12**) für den Rechner (**30**) gekoppelt ist und Daten zwischen einer Chipkarte (**14, 14a**) und der Anschlußschnittstelle (**12**) über die Steuereinheit (**11**) austauschbar sind.

2. Mobilfunktelefon nach Anspruch 1, dadurch gekennzeichnet, daß mit der Steuereinheit (**11**) auch die

anderen für den Mobilfunkverkehr vorhandenen Bauteile verbunden sind, so daß Eingaben über die Tastatur (**16**) oder das Mikrofon speicherbar und über die Anschlußschnittstelle (**12**) weiterleitbar sind bzw. über die Anschlußschnittstelle (**12**) ankommende Daten speicherbar und/oder auf der Anzeige (**15**) anzeigbar sind, wobei die anzuzeigenden Daten durch die Tastatur (**16**) auswählbar sind.

3. Mobilfunktelefon (**10**) nach Anspruch 1 oder 2 mit angekoppeltem Rechner (**30**), dadurch gekennzeichnet, daß der Rechner (**30**) unabhängig vom Mobilfunktelefon (**10**) an ein Kommunikationsnetz (**40**) angeschlossen ist und daß das Mobilfunktelefon (**10**) als angeschlossenes Kartenterminal arbeitend für die Inanspruchnahme von Netzdiensten in dem Kommunikationsnetz (**40**) verwendbar ist.

4. Verfahren zum Betreiben einer aus Mobilfunktelefon (**10**) mit gekoppeltem Rechner (**30**) bestehenden Gerätekombination nach Anspruch 3, dadurch gekennzeichnet, daß vor Inanspruchnahme von ein Kartenterminal erfordernden Netzdiensten zunächst der die Anschlußschnittstelle (**31**) für das Mobilfunktelefon (**10**) steuernde Treiber (**32**) mit der benötigten Treibersoftware geladen wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Treibersoftware über das Kommunikationsnetz (**40**) von einem Server des Mobilfunknetz-Betreibers auf Anforderung in den Treiber (**32**) des Rechners (**30**) geladen wird und daß anhand der Signierung der Treibersoftware mit einem privaten Schlüssel in Verbindung mit dem zugehörigen öffentlichen Schlüssel auf der Chipkarte (**14/14a**) das Vorliegen der berechtigten Treibersoftware automatisch überprüft wird.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß nach Aufbau einer Verbindung vom Rechner (**30**) aus über das Kommunikationsnetz (**40**) zu einem Dienstanbieter (**50**) in Verbindung mit dem Mobilfunktelefon (**10**) als Kartenterminal Chipkartenanwendungen auswählbar und ausführbar sind.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Mobilfunktelefon (**10**) als Kartenterminal des Rechners (**30**) zur Verschlüsselung von sensiblen Daten verwendet wird.

8. Verfahren nach Anspruch 6 und 7, dadurch gekennzeichnet, daß im Rahmen einer laufenden Anwendung benötigte hochsensible Daten wie persönliche Geheimzahl (PIN) oder Geldbeträge über die Tastatur (**16**) des Mobilfunktelefons (**10**) eingegeben und von der Steuereinheit (**11**) in Verbindung mit der Chipkarte (**14**, **14a**) verschlüsselt weitergeleitet werden.

9. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß als Berechtigungsnachweis oder zur Kontrolle auch über das Mikrofon eingegebene Kontrollwörter an die Kontrollinstanz der eröffneten Anwendung weitergeleitet werden, so daß in Verbindung mit hinterlegten Referenzmustern eine Verifizierung des Benutzers durchführbar ist.

10. Verfahren nach einem der Ansprüche 6 bis 9, dadurch gekennzeichnet, daß im Rahmen einer Anwendung vom Rechner (**30**) übernommene Daten an den Speicher (**18**) des Mobilfunktelefons (**10**) weitergeleitet werden.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß die vom Rechner (**30**) übertragenen Daten zur Änderung der Daten in einem Chip der Chipkarte (**14**, **14a**) dienen.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß bei einer als Geldkarte dienenden Chipkarte (**14**, **14a**) die während einer Funkverbindung des Mobilfunktelefons (**10**) eintreffenden Gebührenimpulse eine Abbuchung des entsprechenden Geldbetrages bewirken.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 197 24 901 A1
Int. Cl.[6]: H 04 Q 7/32
Offenlegungstag: 17. Dezember 1998

FIG 1

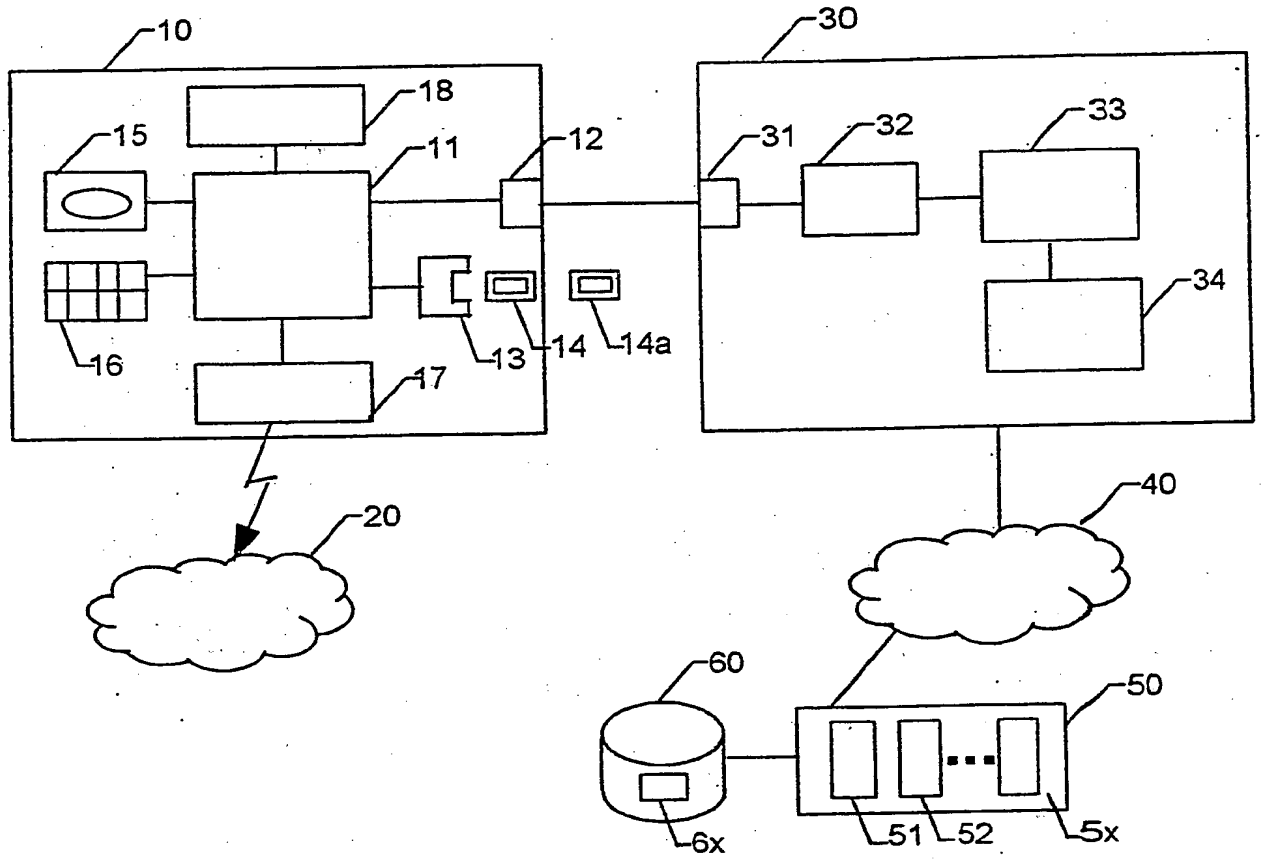


FIG 2